RELIABILITY ANALYSIS OF PHASED MISSIONS

Harald Ziehms

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

RELIABILITY ANALYSIS OF PHASED MISSIONS

by

Harald Ziehms

December 1974

Thesis Advisor J. D. Esary

Approved for public release; distribution unlimited.

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Reliability Analysis of Phased Missions		5. TYPE OF REPORT & PERIOD COVERED Dissertation (December 1974)
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Harald Ziehms		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		12. REPORT DATE December 1974
		13. NUMBER OF PAGES 68
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) Naval Postgraduate School Monterey, California 93940		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

This research was partially supported by the Office of Naval Research (NR042-300) and the Strategic Systems Project Office (TA 19422)
Thesis Advisor: Professor J. D. Esary, Autovon 479-2780

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Reliability - Phased Missions - Multi-Phase Missions - Coherent Systems
Hazard Transform

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

In a phased mission the relevant system configuration (block diagram or fault tree) changes during consecutive time periods (phases). Many systems are required to perform phased missions; a classic example is a spacecraft.

The reliability analysis of a phased mission encounters complexities not present with just one phase, but can be transformed into an analysis of an equivalent synthetic single-phase system. The transformation has a potential for direct application, but can also be used to study refined computational methods and to derive approximations to, and bounds on, mission reliability.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
(Page 1) S/N 0102-014-6601 |

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Reliability Analysis of Phased Missions

by

Harald Ziehms
Korvettenkapitaen, Federal German Navy
Ing. (grad.), Technische Akademie der Luftwaffe, 1966
M.S., Naval Postgraduate School, 1972

Submitted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY

from the
NAVAL POSTGRADUATE SCHOOL
December 1974

ABSTRACT

In a phased mission the relevant system configuration (block diagram or fault tree) changes during consecutive time periods (phases). Many systems are required to perform phased missions; a classic example is a spacecraft.

The reliability analysis of a phased mission encounters complexities not present with just one phase, but can be transformed into an analysis of an equivalent synthetic single-phase system. The transformation has a potential for direct application, but can also be used to study refined computational methods and to derive approximations to, and bounds on, mission reliability.

ACKNOWLEDGEMENTS

This thesis concludes more than four years of graduate studies by the author at the Naval Postgraduate School. They were made possible by the Federal German Navy and the United States Navy.

Members of the faculty, staff, and student body of the Naval Postgraduate School who made these years academically rewarding and personally gratifying, and who provided assistance and encouragement in writing this thesis, are too numerous to be mentioned here individually. Professor James D. Esary, teacher, chairman of the doctoral committee, and thesis advisor; Professor James K. Hartman, Kneale T. Marshall, Joseph J. von Schwind, Fred R. Schwirzke and Karlheinz E. Woehler, members of the doctoral committee; Lieutenant Commander Joseph H. Cyr, Curricular Officer; and Lieutenant Commander William E. Daeschner, Ph.D. candidate and fellow student are noteworthy representatives of these groups. The author wishes to express his gratitude to all of them.

The author also wishes to thank Mrs. Priscilla L. Haney who typed the thesis, and Mrs. Betty Rees who did the drawings.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 BACKGROUND

Among the various areas of applied probability theory and statistics which jointly have become known as reliability theory, structural reliability[1] is the study of qualitative and quantitative relationships between the reliability of (redundant) systems and the reliability of their components. Reliability in the sense used here is the "probability of a device performing its purpose adequately for the period of time intended and the operating conditions encountered."[2]

The problem of constructing reliable systems by using relatively unreliable components redundantly was first studied by von Neumann [1956]. Moore and Shannon [1956], inspired by the von Neumann paper, analyzed relay circuits in which all relays have the same reliability. They proved that the reliability of the circuit is an S-shaped function of the common relay reliability, and subsequently showed that by proper incorporation of redundancy, arbitrarily reliable circuits can be constructed from arbitrarily unreliable elements. Their analysis proceeded from a mathematical result which has come to be called the "Moore-Shannon inequality." Birnbaum, Esary, and Saunders [1961] generalized the concepts and extended some of the results of Moore and Shannon, including the S-shapedness property, to the large class of "coherent" systems,[3] using Boolean functions to describe the functional organization of systems.[4] Esary and Proschan [1963] further extended the Moore-Shannon inequality to the case of unequal component reliabilities, and obtained convenient upper and lower bounds on

system reliability.[5] With the subsequent introduction of the concept of "system life"[6] [Esary and Marshall 1964], a theoretical basis for the reliability analysis of complex systems was complete.

Recent and ongoing research seems to follow mainly two lines. On one hand, the theoretical basis is broadened, more realistic and hence more complex situations are considered, and attempts to do without some of the restrictive assumptions[7] presently required are made. On the other hand, approximation techniques and computational procedures are explored with a view toward their implementation on digital computers.

One specialized area of interest is the extension of the basic problem of structural reliability to the situation in which the functional organization of a system changes with time. This situation, called the phased mission problem, is the topic of this thesis.

1.2 THE PHASED MISSION PROBLEM

The reliability analysis of phased missions has received attention in the basic papers of Rubin [1964] and Weisberg and Schmidt [1966] which present procedures to approximately predict mission reliability and crew safety for manned spacecraft. These authors introduced a method of "cut cancellation"[8] which can be advantageously used to simplify the structure of a system prior to beginning reliability calculations. More recently, a similar approach is described in the United States Navy reliability manual NAVORD OD 29304 Revision A [1973].[9] Muth [1964], in an unpublished report, approached the problem from a different angle, concentrating on "success paths."[10]

The phased mission problem as considered here refers to the following situation:

A <u>system</u> consists of several <u>components</u>. The components perform independently of each other, and each of them can be in one of two states, <u>functioning</u> or <u>failed</u>. No component can be repaired or replaced, and each component <u>has a life</u>.[11] The system performs a <u>mission</u> which can be divided into consecutive time periods, or <u>phases</u>. During each phase it has to accomplish a specified task. Thus the system <u>configuration</u> (a subset of the components and their functional organization which can be represented, for instance, by a block diagram or a fault tree) changes from phase to phase. As is the case with individual components, only two states of the system are recognized, functioning or failed.

With this situation in mind, the problem itself can be stated as:

Given the survival characteristics of the components, the relevant system configuration in each phase, and the duration of the phases, what is the probability that the system will function throughout the mission, i.e. the <u>mission reliability</u> for the system?

The classic example of a phased mission is the voyage of a space vehicle, but many other systems[12] are also required to perform phased missions. To illustrate the ideas and methods of this thesis, the following hypothetical situation[13] will frequently be considered.

<u>Example 1.1</u>. A fire department has three vehicles:

- a multipurpose fire engine (M),
- a tanker (T),
- a light fire truck (L).

The firefighting equipment of a small chemical factory located nearby consists of:

- a sprinkler system (S),
- a hydrant (H),
- a special apparatus for fighting chemical fires (F).

The plant safety engineer wonders whether the combined hardware resources of the fire department and the factory are sufficient to fight a fire in the factory. He consults the fire chief, and together they conclude:

(1) During the initial stage of a fire either the multipurpose engine, which carries a small water supply, or the light truck, provided the sprinkler system works, suffices to evacuate the building.

(2) To contain the fire the factory's special apparatus is needed, together with some auxiliary capability from the multipurpose engine or the light truck. Water can be supplied to the special apparatus and the department's units by the hydrant, or if it is out of order, by the tanker through pumps in the multipurpose engine.

(3) After the fire has been contained it can be controlled either by the special apparatus or the multipurpose engine. Again, water can be supplied by the hydrant or by the tanker together with the multipurpose engine. □

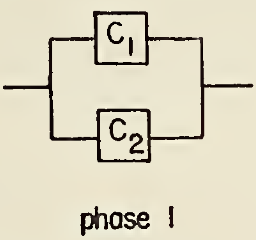
The firefighting system described above has six components, and it has to perform a three-phased mission. If it fails in even one of the three phases, the mission is not accomplished.

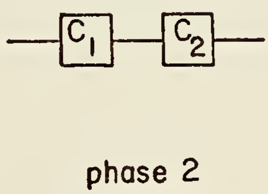
1.3 SOME COMPLEXITIES OF THE PHASED MISSION PROBLEM

The reliability analysis of a phased mission encounters some complexities which are not present when only one phase is considered.

For one thing, it is not correct to do a standard reliability analysis for each phase separately, and then multiply the resulting phase reliabilities together, even if the age of the components at the beginning of each phase is taken into account. The implicit assumption involved, that each component is functioning at the beginning of a phase when the system has functioned throughout the previous phase, is not necessarily true. The following example illustrates this point.

Example 1.2. A system with two independent components, C_1 and C_2, is designed for a two-phased mission. In order for the system to perform the required tasks, at least one component has to function through phase 1 and both components have to function through phase 2. The block diagram for this system is





For $k=1,2$, let π_{k1} denote the probability that component C_k functions through phase 1, and π_{k2} denote the conditional probability that component C_k functions through phase 2, given that it has functioned through phase 1. The system reliability for phase 1 is $\pi_1 = \pi_{11} + \pi_{21} - \pi_{11}\pi_{21}$, and the system reliability for phase 2, given that both the components have functioned through phase 1, is $\pi_2 = \pi_{12}\pi_{22}$. Multiplying these together would lead to the mission reliability

$$\pi = \pi_1 \pi_2 = (\pi_{11} + \pi_{21} - \pi_{11}\pi_{21})\pi_{12}\pi_{22} \ .$$

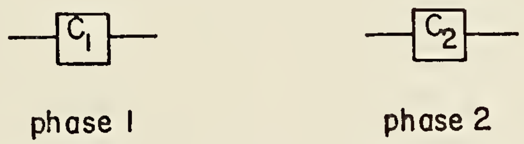
This is greater than the correct mission reliability, which is

$$p = \pi_{11}\pi_{12}\pi_{21}\pi_{22}$$

since mission success is achieved if, and only if, both components function throughout both phases. □

The multi-phase case is potentially different from the single-phase case in another respect. With just one phase, if each component has a life and the system configuration is coherent, then the system has a life.[14] In the multi-phase case this is not necessarily true. Even if all components have lives and all phase configurations are coherent, the system may not have a life. How this can happen is shown in the next example.

Example 1.3. A two-component system is designed for a two-phase mission with the phase configurations represented by the block diagram



If π_{kj}, k=1,2, j=1,2 are defined as in Example 1.2, then there is a probability $(1 - \pi_{11})\pi_{21}\pi_{22}$ that the system fails in phase 1, but functions again in phase 2. In this sense the system does not have a life. □

The possible resurrection of a system in a later phase does not present a problem in the reliability analysis of phased missions if

it is assumed that the life of the system ends at the time of its first failure. This assumption is reasonable since failure of the system in even one phase usually prevents mission success, and will always be made here. By contrast, the possible resurrection of a component would pose a much more serious problem, and is ruled out by the assumption that all components have lives.

1.4 NON-ANALYTIC WAYS TO EVALUATE PHASED MISSIONS

Traditionally, the reliability of complex systems performing multi-phased missions has been estimated by Monte Carlo methods.[15] For large systems, however, mission simulation and determination of success or failure are time-consuming even when digital computers are employed. Furthermore, Monte Carlo methods require a great number of simulation replications before high confidence limits can be placed on a narrow reliability band. It is therefore not surprising that these methods proved to be excessively expensive in terms of both, time and money, especially when parametric studies must be performed.[16]

Another method of analyzing phased missions is by considering the distinct combinations of component performances which lead to mission success, i.e. the <u>success paths</u>. To see how this works, assume that the system has n components $C_1,\ldots,C_n$, and is designed for an m-phased mission. Let ℓ_k be the maximum number of phases component C_k survives, $\ell_k=0,1,\ldots,m$, $k=1,\ldots,n$. Each of the n-tuples $(\ell_1,\ldots,\ell_n)$ then represents an event which implies either mission success or failure, depending on the functional organization of the system in the m phases. The probabilities of the events can be computed from the component survival characteristics. Since the events

are disjoint, the probability of mission success, i.e. the reliability of the system for the mission, is the sum of the probabilities of the success path events.

This method is straightforward and could easily be developed into an algorithm for computer implementation. In addition, it has the advantage that with a slight modification not only the mission reliability but also the probability of the system to survive the first j phases of its mission, $j=1,\ldots,m$, can be obtained. However, the number of n-tuples to be considered, $(m+1)^n$, is such that economic reasons prevent its use even for moderately sized systems performing only a few phases.

A refined computational method based on success paths was developed by Muth [1964]. His approach consists of setting up phase matrices of components and success paths, and collapsing these matrices successively into a single matrix which represents system success at the end of phase j, $j=1,\ldots,m$. If the system can be broken up into many small subsystems which have no components in common and thus can be analyzed separately, this approach makes reliability computations feasible.

1.5 CONTENTS AND SUMMARY

In this thesis, the phased mission problem is approached analytically. The verbal statement of the problem in Section 1.2 is translated into mathematical terms in Chapter 2. The resulting model is an equation which relates mission reliability to the survival characteristics of the components, the phase durations, and the phase configurations. However, this equation, i.e. 2.3.1, neither provides much insight into the problem nor can it easily be used to obtain numerical results.

In Chapter 3 a transformation is exhibited by means of which a multi-phase mission can be reduced to an equivalent synthetic single-phase system. Direct applications of this transformation are discussed in Chapter 4. They include a method to adapt existing algorithms and computer programs to the calculation of exact mission reliabilities, and a technique to simplify phased mission problems prior to beginning reliability calculations.

A troublesome byproduct of the transformation is an apparent increase in the number of components of the system to which it is applied. This may aggravate computational problems and make the calculation of the exact mission reliability infeasible. Consequently, it may be necessary to resort to approaches which require less computational effort. Chapter 5, therefore, is devoted to a study of bounds on mission reliability. Several upper and lower bounds are derived and compared with each other, both in terms of precision and the amount of computational effort required, and an algorithm for the "best" lower bound is presented. An approximation technique which has successfully been applied to single-phase systems is based on the approximate hazard transform of Esary and Hayne [1973]; its potential for the phased mission problem is discussed in Chapter 6.

Finally, possible extensions of the methods presented in this thesis, and areas where further research is needed, are indicated in Chapter 7.

2. MATHEMATICAL FORMULATION OF THE PHASED MISSION PROBLEM

The starting point of an analysis of the phased mission problem described in Section 1.2 is a mathematical model which quantitatively relates the variables of interest (the survival characteristics of the components, the functional organization of these components in the various phases of the mission, and the duration of the phases) to mission reliability. Such a model is developed here in three steps. The analytic tools employed are extensions of those used in standard reliability analysis. The underlying assumptions are made explicit.

2.1 A MODEL FOR COMPONENT PERFORMANCES

The system under consideration is assumed to have n components, labelled $C_1,\ldots,C_n$. Each component C_k has a life, and hence its time to failure, or life length, is well defined. Since it depends on many factors and cannot be predicted accurately, it is expressed by a non-negative random variable[17] T_k. The assumption[18] that the components perform independently of each other formally means that $T_1,\ldots,T_n$ are stochastically independent.

For each component C_k and all times $t\geq 0$, let $X_k(t)$ be a Bernoulli random variable defined by

$$X_k(t) = \begin{cases} 1 \text{ if component } C_k \text{ functions at time } t, \\ 0 \text{ otherwise.} \end{cases}$$

The random variable $X_k(t)$ is called a performance state indicator variable, and the stochastic process $\{X_k(t),t\geq 0\}$ is the performance process of the component C_k. Since each component has a life, this process has the properties:

(2.1.1)

a) $X_k(t) = 0 \iff X_k(s) = 0, \; s > t.$

b) $X_k(t) = 1 \iff X_k(s) = 1, \; 0 \le s \le t.$

Thus a sample path of a performance process is non-increasing and continuous from the right, as indicated in Figure 2.1.

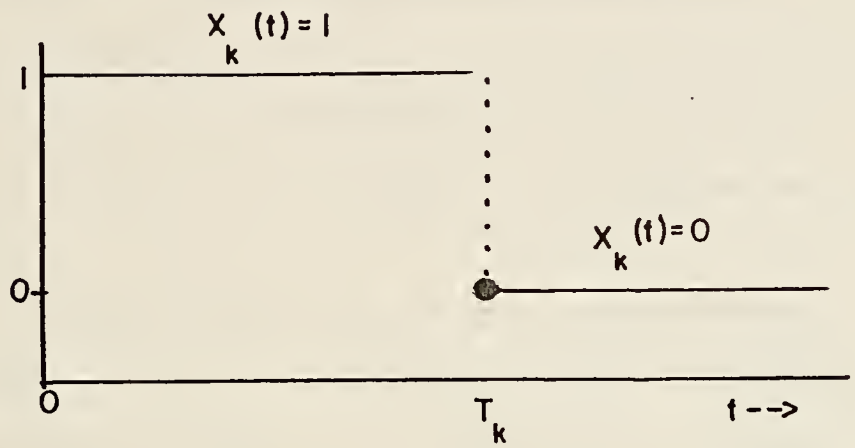


Figure 2.1. Performance process sample path, component C_k.

For each $t \ge 0$, let $\underset{\sim}{X}(t) = (X_1(t), \ldots, X_n(t))$ be the <u>performance state indicator vector</u> of the set of components. Then the stochastic process $\{\underset{\sim}{X}(t), t \ge 0\}$ is called the <u>joint performance process</u> of the components.

The joint performance process is a mathematical description of the component failure times, and as such the first step in the development of the model. It is compatible with the use of structure functions to represent system configuration within the phases, which is discussed in the next section.

2.2 A MODEL FOR SYSTEM CONFIGURATIONS

It is assumed throughout this thesis that the state of the system (i.e. functioning or failed) is completely determined by the states of

its components.[19] Then the system configuration in each of the phases can be described by a block diagram[20] or a fault tree[21] for conceptual purposes, or by a structure function for mathematical analysis. A structure function is a binary function ϕ of binary variables $x_1,\ldots,x_n$ which relates the performance state of the system to the performance states of its components; in particular $\phi(\underset{\sim}{x}) = \phi(x_1,\ldots,x_n) = 1$ if the system functions, and $\phi(\underset{\sim}{x}) = 0$ otherwise, where $x_k = 1$ if component C_k functions, and $x_k = 0$ otherwise.

It is further assumed that each phase configuration of a system is coherent,[22] i.e. can be represented by a block diagram or a fault tree using AND and OR gates. If a configuration is coherent, then its structure function ϕ has the properties:[23]

(2.2.1)

a) $\phi(\underset{\sim}{x}) \geq \phi(\underset{\sim}{y})$ whenever $x_k \geq y_k$, $k=1,\ldots,n$.

b) $\phi(\underset{\sim}{0}) = \phi(0,\ldots,0) = 0$.

c) $\phi(\underset{\sim}{1}) = \phi(1,\ldots,1) = 1$.

To illustrate, a block diagram for the mission described in Example 1.1 is shown in Figure 2.2, and a fault tree in Figure 2.3.

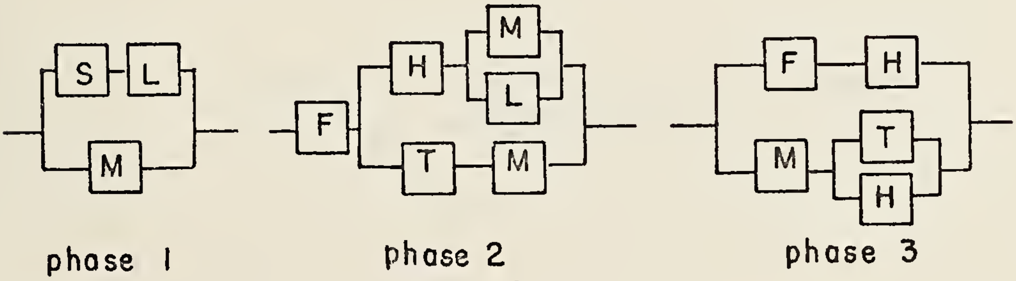


Figure 2.2. Block diagram for the mission of Example 1.1.

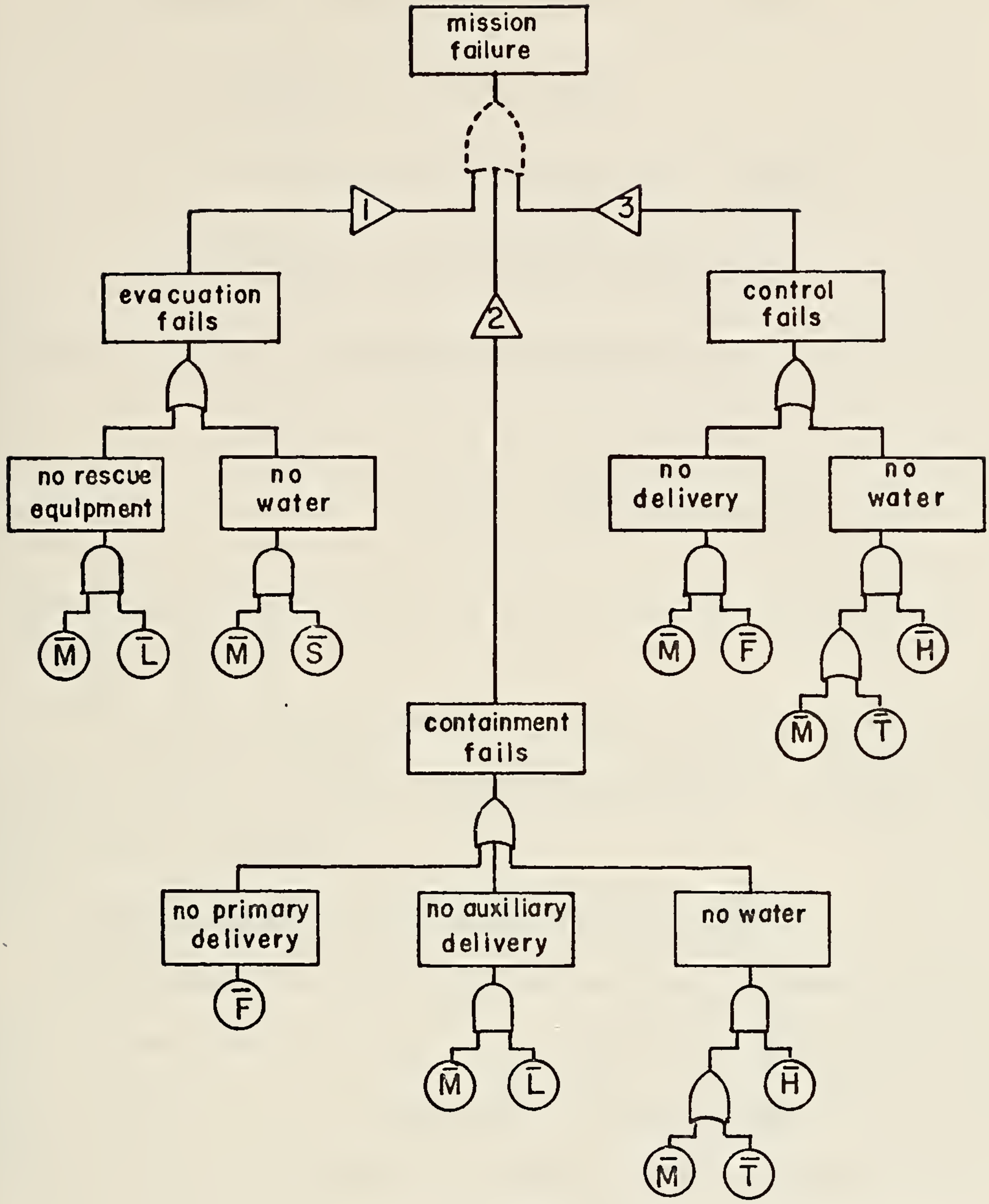


Figure 2.3. Fault tree for the mission of Example 1.1.

The structure functions for the system of Example 1.1 are:

for phase 1, $\phi_1 = x_M \vee x_L x_S$,

for phase 2, $\phi_2 = x_F(x_H(x_M \vee x_L) \vee x_M x_T)$,

for phase 3, $\phi_3 = x_F x_H \vee x_M(x_T \vee x_H)$.

The symbol $\vee$ is the arithmetic OR operator, i.e.

$$x_1 \vee x_2 = \begin{cases} 1 \text{ if } x_1 = 1 \text{ or } x_2 = 1, \\ 0 \text{ if } x_1 = 0 \text{ and } x_2 = 0, \end{cases}$$

or for computational purposes, $x_1 \vee x_2 = x_1 + x_2 - x_1 x_2 = 1 - (1-x_1)(1-x_2)$.

The phase structure functions can be combined with the joint performance process to achieve a concise mathematical formulation of the phased mission problem.

2.3 A COMPLETE MODEL FOR THE PHASED MISSION PROBLEM

The mission is assumed to be divided into m phases, and to start at time $t=0$. For $j=1,\ldots,m$, the time at which phase j ends and, except for $j=m$, the next phase begins, is denoted by t_j. The structure function appropriate for phase j is denoted by ϕ_j.

The event that the system functions during phase j can be expressed as $\{\phi_j(\underset{\sim}{X}(t_j))=1\}$, and the event that the system functions throughout the m phases, i.e. throughout the mission, as $\{\phi_1(\underset{\sim}{X}(t_1))=1,\ldots,\phi_m(\underset{\sim}{X}(t_m))=1\}$. The <u>mission reliability</u> for the system is the probability that this event occurs. Since $\phi_j(\underset{\sim}{X}(t_j))$, $j=1,\ldots,m$, are Bernoulli random variables, this probability can be expressed compactly by

$$(2.3.1) \qquad p = P[\prod_{j=1}^{m} \phi_j(\underset{\sim}{X}(t_j))=1] = E \prod_{j=1}^{m}\phi_j(\underset{\sim}{X}(t_j)),$$

where E denotes expectation.

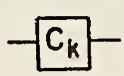
Equation (2.3.1) is the complete model for the phased mission problem as described in the introduction and as qualified by the assumptions made, but neither is it a formula for practical reliability calculations nor does it provide much insight into the problem. It does, however, indicate that the sequential operation of the phase configurations to some extent resemble the operation of subsystems performing in series. This fact is essential in transforming the phased mission problem.

3. TRANSFORMATION OF THE PHASED MISSION PROBLEM

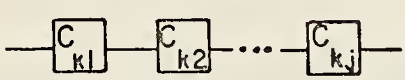
Complexities in the reliability analysis of phased missions arise because a component's performance in one phase is not stochastically independent of its performance in any other phase. The dependence, however, is of a special type. A component functions in phase j if, and only if, it has previously functioned in phase 1, and in phase 2, ..., and in phase $j-1$, and then functions in phase j. This sequence of requirements suggests that the performance of a component in phase j can be represented by a series-like structure whose elements represent its performance in phases $1,...,j$.

3.1 THE TRANSFORMATION

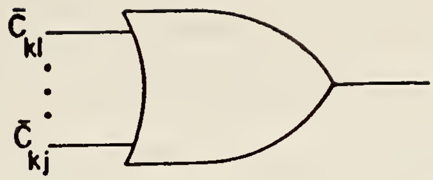
Suppose that component C_k is replaced in phase j by a system of components $C_{k1},...,C_{kj}$, performing independently and in series. In block diagram format, the block



is replaced in phase j by the system



In fault tree format, the input event $\bar{C}_k$ (failure of component C_k) is replaced in phase j by



Let $U_{k1},\ldots,U_{kj}$ be independent performance state indicator variables for the components $C_{k1},\ldots,C_{kj}$, with

$$
\begin{aligned}
& P[U_{k1}=1] = P[X_k(t_1)=1] \\
(3.1.1) \qquad & \\
& P[U_{ki}=1] = P[X_k(t_i)=1 \mid X_k(t_{i-1})=1], \ i=2,\ldots j.
\end{aligned}
$$

Then $P[X_k(t_j)=1] = P[U_{k1}U_{k2}\cdots U_{kj}=1]$, and thus

$$X_k(t_j) =^{st} U_{k1}U_{k2}\cdots U_{kj},$$

where $=^{st}$ means "is stochastically equal to" or, less formally, "has the same distribution as." Thus the original component and the substituted system have, as of the end of phase j, the same reliability.

The preceeding observations suggest that a <u>transformation</u> of the phased mission problem can be accomplished by

a) Replacing, in the configuration for phase j, $j=1,\ldots,m$, component C_k, $k=1,\ldots,n$, by a series system in which the components $C_{k1},\ldots,C_{kj}$ perform independently, with the probabilities of functioning given in (3.1.1).

b) Considering the transformed phase configurations to be subsystems which operate in series.

The resulting new system, which has (at most) n*m independent components, is the equivalent system. As will be shown later, the ordinary reliability of the equivalent system is the same as the reliability of the original system for its phased mission.

The block diagram for the equivalent system arising out of Example 1.1 is given in Figure 3.1. A comparison with the block diagram for the phased mission shown in Figure 2.2 illustrates how the transformation is implemented.

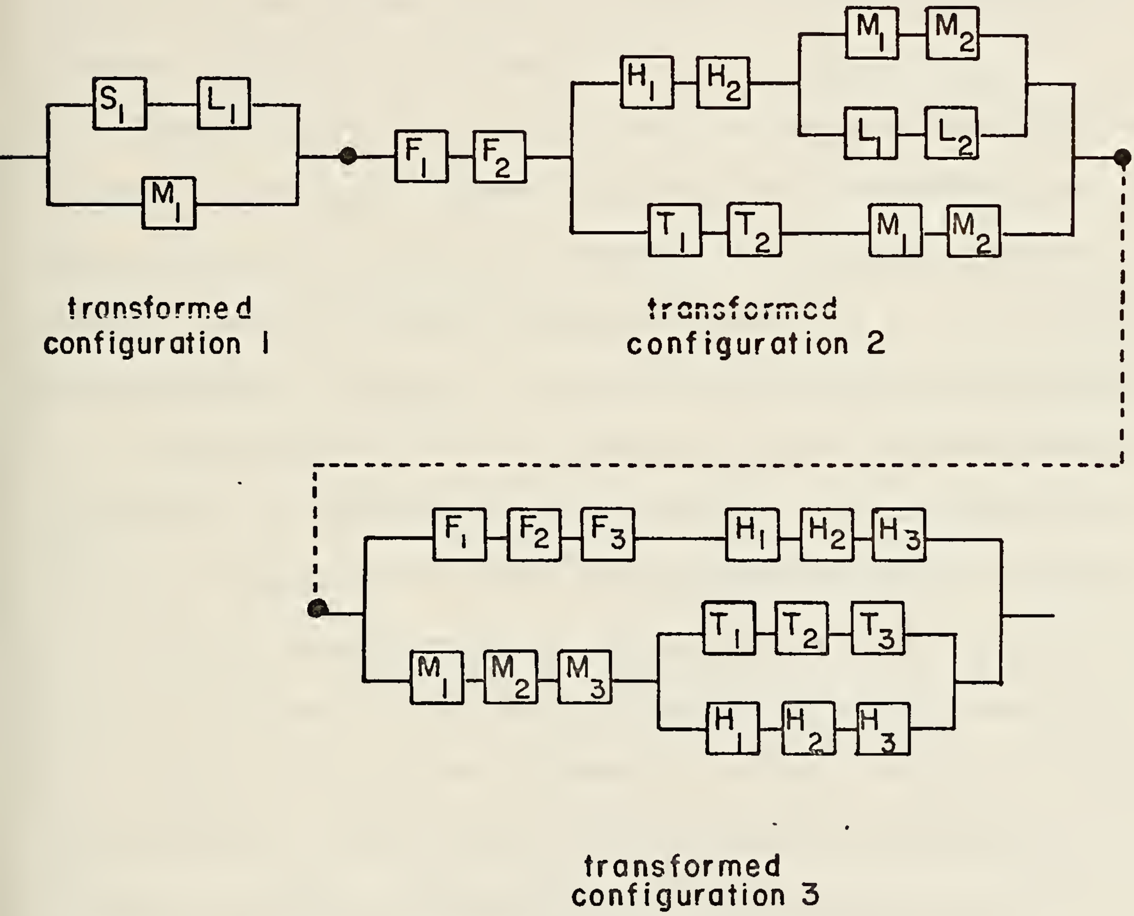


Figure 3.1. Equivalent system for the mission of Example 1.1.

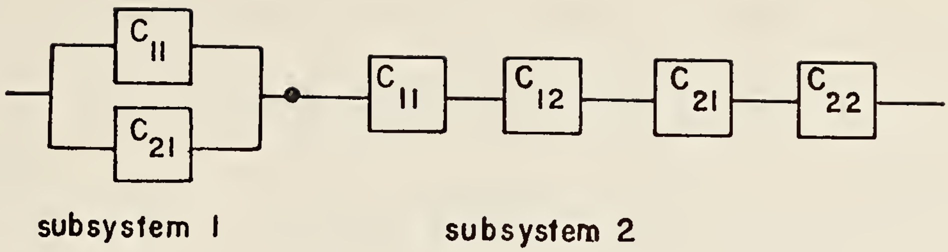
3.2 SOME PROPERTIES OF THE EQUIVALENT SYSTEM

Two important properties of the equivalent system are that it performs just one phase, and that it is coherent. The former is a direct consequence of step (b) of the transformation. To obtain the latter, note that by step (b) of the transformation the equivalent system is a series, and hence coherent, structure of subsystems which themselves are coherent structures by assumption; their elements are, from step (a) of the transformation, series systems of components. The result then follows from the fact that a coherent structure of coherent structures is coherent.[24]

These two properties together with the assumption that all components in the original system - and hence all components in the equivalent system - have lives imply that the equivalent system has a life.[25] Thus the potential difficulties mentioned in the introduction and illustrated in Example 1.3 cannot occur in the equivalent system.

By contrast, another one of the difficulties of phased missions mentioned in the introduction does not disappear in the equivalent system. Although the m phase configurations operating in sequence in the phased mission become m subsystems operating in series in the equivalent system - a fact which simplifies the problem considerably - the subsystems usually have components in common[26] and do not function independently. Hence the product of the subsystem reliabilities is in general not equal to the reliability of the equivalent system, as is illustrated by the following extension of Example 1.2.

Example 3.1. For the mission described in Example 1.2, the equivalent system has the block diagram

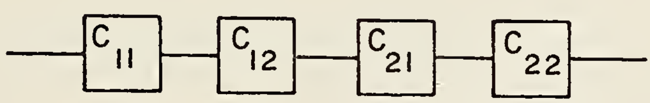


Letting π_{kj}, $k=1,2$, $j=1,2$, be as defined in Example 1.2, and $\rho_{k1}=\pi_{k1}$, $\rho_{k2}=\pi_{k1}\pi_{k2}$, $k=1,2$, the subsystem reliabilities are

$$\rho_1 = \pi_{11} + \pi_{21} - \pi_{11}\pi_{21} = \rho_{11} + \rho_{21} - \rho_{11}\rho_{21},$$

$$\rho_2 = \pi_{11}\pi_{12}\pi_{21}\pi_{22} = \rho_{12}\rho_{22}.$$

Their product $\rho_1\rho_2$ is, except in trivial cases, less than the true system reliability $p = \pi_{11}\pi_{12}\pi_{21}\pi_{22} = \rho_{12}\rho_{22}$ which can be found by reducing the block diagram to its simplest form



The true reliability for the equivalent system does agree with the reliability for the phased mission given in Example 1.2. □

3.3 MATHEMATICAL FORMULATION OF THE TRANSFORMED PROBLEM

The transformed version of the phase j configuration functions if the event $\{\phi_j(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)})=1\}$ occurs, where $\underset{\sim}{U}^{(i)}=(U_{1i},\ldots,U_{ni})$, and $\underset{\sim}{U}^{(i)}\underset{\sim}{U}^{(k)}=(U_{1i}U_{1k},\ldots,U_{ni}U_{nk})$. The equivalent system functions if the event

$$\{\phi_1(\underset{\sim}{U}^{(1)}) = 1,\ \phi_2(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}) = 1, \ldots, \phi_m(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(m)}) = 1\}$$

occurs. Thus the reliability of the equivalent system is

$$\begin{aligned} p &= P[\textstyle\prod_{j=1}^{m}\phi_j(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)}) = 1] \\ &= E\ \textstyle\prod_{j=1}^{m}\phi_j(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)}). \end{aligned} \tag{3.3.1}$$

3.4 RELIABILITY EQUIVALENCE OF THE ORIGINAL AND THE EQUIVALENT SYSTEM

It remains to establish that the reliability of the equivalent system agrees with the mission reliability of the original system, i.e. that p as given by (3.3.1) agrees with p as given by (2.3.1). This is done by the following theorem and the subsequent remarks.

Theorem 3.1. Let $X_1,\ldots,X_m$ be a non-increasing sequence of Bernoulli random variables, i.e. $X_1 \geq X_2 \geq \ldots \geq X_m$. Let $U_1,\ldots,U_m$ be independent Bernoulli random variables with

$$P[U_1=1] = P[X_1=1],$$

$$P[U_j=1] = P[X_j=1|X_{j-1}=1],\ j=2,\ldots,m.$$

Then $X_1,\ldots,X_m \overset{st}{=} U_1, U_1U_2, \ldots, U_1U_2\ldots U_m$.

Proof. It is only necessary to show for each non-increasing binary sequence $x_1 \geq x_2 \geq \ldots \geq x_m$, $x_j=0$ or 1, $j=1,\ldots,m$, that

$$P[X_1=x_1,\ldots,X_m=x_m] = P[U_1=x_1, U_1U_2=x_2, \ldots, U_1U_2\ldots U_m=x_m].$$

For the sequence $x_1=0, x_2=0, \ldots, x_m=0$,

$$\begin{aligned} P[X_1=0,\ldots,X_m=0] &= P[X_1=0] = P[U_1=0] \\ &= P[U_1=0, U_1U_2=0, \ldots, U_1U_2\ldots U_m=0]. \end{aligned}$$

For the sequence $x_1=1,\ x_2=1,\ldots,x_m=1$,

$$P[X_1=1,\ldots,X_m=1] = P[X_m=1|X_{m-1}=1]\ldots$$

$$\ldots P[X_2=1|X_1=1]\ P[X_1=1]$$

$$= P[U_m=1]\ldots P[U_2=1]\ P[U_1=1]$$

$$=P[U_1=1,U_1U_2=1,\ldots,U_1U_2\ldots U_m=1].$$

For any other sequence $x_j=1,\ j=1,\ldots,\ell,\ x_j=0,\ j=\ell+1,\ldots,m$,

$$P[X_1=1,\ldots,X_\ell=1,X_{\ell+1}=0,\ldots,X_m=0]$$

$$= P[X_m=0,\ldots,X_{\ell+1}=0|X_\ell=1,\ldots,X_1=1]\ P[X_\ell=1,\ldots,X_1=1]$$

$$= P[X_{\ell+1}=0|X_\ell=1]\ P[X_\ell=1,\ldots,X_1=1]$$

$$= P[U_{\ell+1}=0]\ P[U_\ell=1,\ldots,U_1=1]$$

$$= P[U_1=1,\ldots,U_\ell=1,U_{\ell+1}=0]$$

$$= P[U_1=1,U_1U_2=1,\ldots,U_1U_2\ldots U_\ell=1,$$

$$U_1\ldots U_\ell U_{\ell+1}=0,\ldots,U_1U_2\ldots U_m=0].\ \square$$

From (2.1.1) the sequence of variables $X_k(t_1),\ldots,X_k(t_m)$, which indicate the performance of component C_k at the end of each phase, is non-increasing. Thus for $U_{k1},\ldots,U_{km}$ constructed according to (3.1.1),

$$X_k(t_1),X_k(t_2),\ldots,X_k(t_m) \overset{st}{=} U_{k1},U_{k1}U_{k2},\ldots,U_{k1}U_{k2}\ldots U_{km}.$$

Then, since component failure times, and consequently performance processes, are independent,

$$\underset{\sim}{X}(t_1),\underset{\sim}{X}(t_2),\ldots,\underset{\sim}{X}(t_m) =^{st} \underset{\sim}{U}^{(1)},\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)},\ldots,\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(m)}.$$

Since the event "success in the phased mission" occurs if $\phi_j(\underset{\sim}{X}(t_j))=1$, $j=1,\ldots,m$, and the event "functioning of the equivalent system" occurs if $\phi_j(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)})=1$, $j=1,\ldots,m$, then these two events are stochastically equivalent. Thus p as given by (2.3.1) agrees with p as given by (3.3.1).

4. DIRECT APPLICATIONS OF THE TRANSFORMATION

The transformation described in Chapter 3 can be used to obtain results for the phased mission problem which are of theoretical and practical interest. Two of these are discussed below.

4.1 CALCULATION OF THE EXACT MISSION RELIABILITY

Several computational methods[27] are known for the numerical evaluation of system reliability in the single-phase case. Based on them, computer programs[28] for reliability analyses have been developed. The transformation provides, in principle, a way to adapt these methods and programs to the calculation of mission reliabilities in the multi-phase case. The necessary inputs are the phase configurations and, phase by phase, the conditional probabilities that the components survive the phase, given that they have survived the previous phases, i.e. the conditional component phase reliabilities

$$\pi_{k1} = P[X_k(t_1)=1],$$
$$\pi_{kj} = P[X_k(t_j)=1 \mid X_k(t_{j-1})=1], \quad j=2,\dots,m, \tag{4.1.1}$$

$k=1,\dots,n$. From (3.1.1) the conditional component phase reliabilities are the reliabilities of the components in the equivalent system. Computer programs could be adapted to accomplish steps (a) and (b) of the transformation internally, and then to find the reliability of the equivalent system which by Theorem 3.1 is the mission reliability for the original system.

Theoretically, this approach eliminates all difficulties inherent in the phased mission problem, because it reduces the reliability

analysis of a system performing a multi-phase mission to the standard reliability analysis of a single-phase system. It may, however, not always be a practical or an efficient approach. Realistic systems usually have so many components to start with that when the transformation is performed with its concomitant increase in the number of components in the equivalent system, the costs - in terms of computer time and memory - of calculating exact mission reliabilities are excessive. Frequently this is the case even for single-phase missions. Most existing reliability analysis programs therefore are designed to provide only approximations to system reliability, and it is not always clear whether such an approximation is conservative or optimistic. Thus the direct approach, i.e. applying the transformation and then using an existing computer program, is not necessarily the best solution to the phased mission problem.

Different approaches to the assessment of mission reliability which avoid some of the problems mentioned above will be discussed in Chapters 5 and 6, after an additional direct application of the transformation has been presented.

4.2 THE CUT CANCELLATION TECHNIQUE

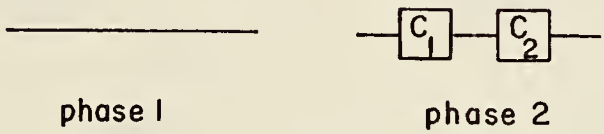
The transformation can provide a simple rationale for the cut cancellation technique of Rubin, Weisberg, and Schmidt. Conversely, cut cancellation can result in an advantageous simplification of the earlier configurations of a phased mission, prior to any implementation of the transformation.

For instance, the sequence of phase configurations in Example 1.2 turned out to have the mission reliability $p = \pi_{11}\pi_{12}\pi_{21}\pi_{22}$. Using

notation introduced in Example 3.1, i.e. defining the (unconditional) component reliability ρ_{kj} as the probability that component C_k survives from the beginning of the mission through the end of phase j,

(4.2.1) $$\rho_{kj} = P[X_k(t_j)=1] = \prod_{i=1}^{j} \pi_{ki}, \quad j=1,\ldots,m,$$

$k=1,\ldots,n$, this mission reliability can be written as $p = \rho_{12}\rho_{22}$. The sequence of phase configurations



has the same mission reliability. In Example 1.2 the only minimal cut set in phase 1, $\{C_1,C_2\}$, contains the phase 2 cut sets $\{C_1\}$ and $\{C_2\}$. Thus $\{C_1,C_2\}$ can be "cancelled" in its phase, leaving a configuration which can never fail.

The minimal cut sets of a (coherent) system are the minimal (in the sense of set inclusion) combinations of components which by all failing cause the system to fail. Every coherent system can be viewed as a series structure of subsystems, each of which consists of the components in a minimal cut set acting in parallel.[29] Equivalently, the configuration of every coherent system - and, in the context of the phased mission problem, every phase configuration - can be described by a complete list of its minimal cut sets.

The rule for cut cancellation is:

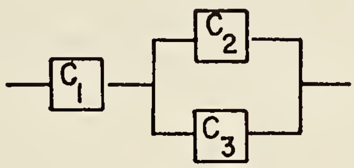
> A minimal cut set in a phase can be cancelled, i.e. omitted from the list of minimal cut sets for that

phase, if it contains a minimal cut set of a

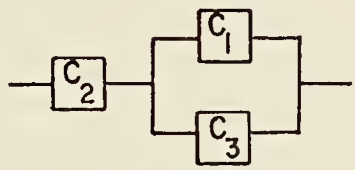
later phase.

A slightly more typical illustration of how cut cancellation works is given in the following example.

<u>Example</u> <u>4.1</u>. A mission has the phase configurations



phase 1



phase 2

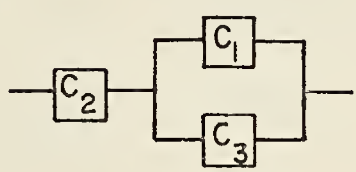
The minimal cut sets are: in phase 1 $\{C_1\}$ $\{C_2,C_3\}$,

in phase 2 $\{C_2\}$ $\{C_1,C_3\}$.

The phase 1 cut $\{C_2,C_3\}$ contains the phase 2 cut $\{C_2\}$, and so can be cancelled in phase 1. No cancellation results from the fact that the phase 2 cut $\{C_1,C_3\}$ contains the phase 1 cut $\{C_1\}$ because cut cancellation is not a symmetric procedure.

After cancellation the sequence of phase configurations reduces to

phase 1



phase 2

It is easy to verify that both sequences lead to the same mission reliability by comparing their equivalent systems. □

The use of cut cancellation is justified by the theorem below. In its proof, the symbol V is the repeated OR operator; for binary variables $x_1,\ldots,x_n$,

$$V_{k=1}^{n} x_k = x_1 \vee x_2 \vee \ldots \vee x_n,$$

or, for computational purposes,

$$V_{k=1}^{n} x_k = 1 - \prod_{k=1}^{n} (1-x_k).$$

<u>Theorem 4.1</u>. Cut cancellation does not affect mission reliability.

<u>Proof</u>. Assume without loss of generality that a system performing a phased mission contains a minimal cut set $\{C_1,\ldots,C_r,C_{r+1},\ldots,C_s\}$ in the configuration of phase h, and a minimal cut set $\{C_1,\ldots,C_r\}$ in the configuration of phase i, $i>h$. From (3.3.1) the reliability of the equivalent system is, in shorthand notation,

$$p = E\ \phi_1\phi_2\ldots\phi_h\ldots\phi_i\ldots\phi_m.$$

Let $\bar{\phi}_h$ and $\bar{\phi}_i$ denote the structure functions of the subsystems that remain when the above minimal cut sets are omitted in the transformed configurations of phase h and phase i, respectively. Then

$$\phi_h = \bar{\phi}_h * (V_{k=1}^{s} \prod_{j=1}^{h} U_{kj}),$$

(4.2.2)

$$\phi_i = \bar{\phi}_i * (V_{k=1}^{r} \prod_{j=1}^{i} U_{kj}).$$

The reliability can now be expressed as

$$p = E\ \phi_1\phi_2\cdots\phi_h^{-}*(V_{k=1}^{s}\prod_{j=1}^{h}U_{kj})\cdots\phi_i^{-}*(V_{k=1}^{r}\prod_{j=1}^{i}U_{kj})\cdots\phi_m$$

$$= E\ \phi_1\phi_2\cdots\phi_h^{-}\cdots\phi_i^{-}\cdots\phi_m*(V_{k=1}^{s}\prod_{j=1}^{h}U_{kj})(V_{k=1}^{r}\prod_{j=1}^{i}U_{kj}).$$

By the laws of Boolean algebra,

$$(V_{k=1}^{s}\prod_{j=1}^{h}U_{kj})(V_{k=1}^{r}\prod_{j=1}^{i}U_{kj})$$

$$= V_{k=1}^{r}[(\prod_{j=1}^{i}U_{kj})(1\ v\ V_{\ell=1,\ell\neq k}^{s}\prod_{j=1}^{h}U_{kj})]$$

$$= V_{k=1}^{r}\prod_{j=1}^{i}U_{kj}.$$

Therefore,

$$p = E\ \phi_1\phi_2\cdots\phi_h^{-}\cdots\phi_i^{-}*(V_{k=1}^{r}\prod_{j=1}^{i}U_{kj})\cdots\phi_m$$

$$= E\ \phi_1\phi_2\cdots\phi_h^{-}\cdots\phi_i\cdots\phi_m,$$

i.e. the minimal cut set can be omitted from the transformed configuration of phase h without changing the reliability of the equivalent system.[30] The result then follows from Theorem 3.1. □

Remark 4.2. An even stronger result than Theorem 4.1 can be achieved. If (as henceforth will be done) ϕ_j^{-} is used to denote the structure function of the phase j configuration after cut cancellation has been performed to the greatest possible extent, $j=1,\ldots,m$, then by an argument along the lines of the proof above it can be shown that

(4.2.3) $$\prod_{j=1}^{m}\phi_j^{-} = \prod_{j=1}^{m}\phi_j,$$

although it follows from (4.2.2) that for $j=1,\ldots,m$,

(4.2.4) $$\phi_j^{-} \geq \phi_j,$$

and strict inequality may hold in (4.2.4) for all j except $j=m$. □

As a final illustration of the cut cancellation technique, consider its effect on the mission described in Example 1.1. The minimal cut sets for this mission are, before cancellation:

in phase 1 {M,L} {M,S}

in phase 2 {F} {H,M} {H,T} {M,L}

in phase 3 {F,M} {H,M} {H,T}

The minimal cut sets remaining after cancellation are:

in phase 1 {M,S}

in phase 2 {F} {M,L}

in phase 3 {F,M} {H,M} {H,T}

A block diagram for the sequence of simplified phase configurations is shown in Figure 4.1.

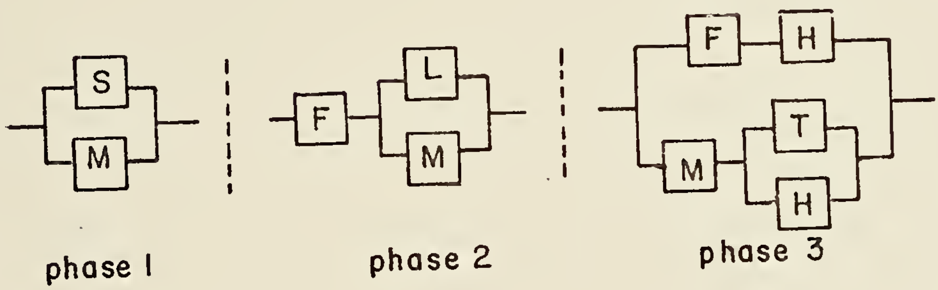


Figure 4.1. Block diagram for the mission of Example 1.1 after cut cancellation.

After cancellation, the transformation can be applied to obtain the equivalent system shown in Figure 4.2. This system is considerably simpler than the one shown in Figure 3.1, but has the same reliability. Reliability computations are simplified accordingly.

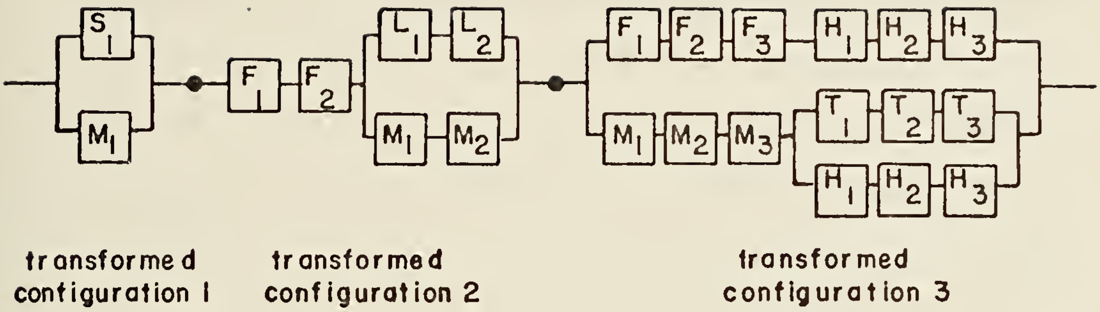


Figure 4.2. Equivalent system for the mission of Example 1.1, after cancellation.

5. BOUNDS ON MISSION RELIABILITY

In Section 4.1 it was shown how the transformation can be used directly for the calculation of exact mission reliabilities; it was also pointed out why this approach may be problematic. In this chapter, <u>bounds</u> on mission reliability are studied. Bounds require less computational effort than the exact reliabilities and, although not necessarily precise, often suffice for the purpose at hand.

5.1 BOUNDS BASED ON PHASE RELIABILITY FUNCTIONS

A tempting procedure to approximate mission reliability is to deliberately commit what was shown[31] to be a logical error when trying to find exact reliabilities, namely to compute the reliability of each phase configuration separately, and then to multiply the results together. There are at least two choices of component reliabilities to use in doing this: the conditional component phase reliabilities π_{kj} given in (4.1.1), or the (unconditional) component reliabilities ρ_{kj} given in (4.2.1). The first choice leads to estimating mission reliability by

$$\pi_{PRF} = \prod_{j=1}^{m} h_j(\pi_{1j},\ldots,\pi_{nj}), \tag{5.1.1}$$

and the second choice to estimating mission reliability by

$$\rho_{PRF} = \prod_{j=1}^{m} h_j(\rho_{1j},\ldots,\rho_{nj}), \tag{5.1.2}$$

where in both cases h_j, $j=1,\ldots,m$, are the reliability functions for the phase configurations.[32] The <u>reliability function</u> of a system with structure function ϕ is defined by

$$h(p_1,\ldots,p_n) = P[\phi(X_1,\ldots,X_n)=1] = E\phi(X_1,\ldots,X_n),$$

where $X_1,\ldots,X_n$ are independent performance state indicator variables with $P[X_k=1] = p_k$, $k=1,\ldots,n$.

The following theorem shows that (5.1.1) gives an optimistic result (cf. Example 1.2), i.e. is an <u>upper</u> bound on mission reliability, and that (5.1.2) gives a conservative result (cf. Example 3.1), i.e. is a <u>lower</u> bound.

<u>Theorem 5.1</u>. For π_{PRF} as given by (5.1.1), ρ_{PRF} as given by (5.1.2), and p as given by (2.3.1) or (3.3.1), $\rho_{PRF} \le p \le \pi_{PRF}$.

<u>Proof</u>. The coherent phase configurations have non-decreasing structure functions from (2.2.1), and $\underset{\sim}{U}^{(1)},\ldots,\underset{\sim}{U}^{(m)}$ are independent by construction. Thus

$$\begin{aligned} E \prod_{j=1}^{m}\phi_j(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)}) &\le E \prod_{j=1}^{m}\phi_j(\underset{\sim}{U}^{(j)}) \\ &= \prod_{j=1}^{m}E\phi_j(\underset{\sim}{U}^{(j)}), \end{aligned} \tag{5.1.3}$$

so that $p \le \pi_{PRF}$ from (3.3.1) and (5.1.1).

The proof that $\rho_{PRF} \le p$ uses standard properties[33] of associated[34] random variables. Since U_{kj}, $k=1,\ldots,n$, $j=1,\ldots,m$, are independent and thus associated, and ϕ_j, $j=1,\ldots,m$, are non-decreasing, then $\phi_j(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)})$, $j=1,\ldots,m$, are associated. Therefore the inequality

$$\prod_{j=1}^{m}E\phi_j(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)}) \le E \prod_{j=1}^{m}\phi_j(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)})$$

holds, so that $\rho_{PRF} \le p$ from (3.3.1) and (5.1.2). □

The method of approximating mission reliability described above can also be employed after cut cancellation has been performed. Denoting the phase reliability functions of the simplified phase configurations

by h_j^-, $j=1,\ldots,m$, the resulting approximations[35] corresponding to π_{PRF} and ρ_{PRF} are

$$(5.1.4) \qquad \pi_{PRF-CC} = \prod_{j=1}^{m} h_j^-(\pi_{1j},\ldots,\pi_{nj})$$

and

$$(5.1.5) \qquad \rho_{PRF-CC} = \prod_{j=1}^{m} h_j^-(\rho_{1j},\ldots,\rho_{nj}),$$

respectively. Again, π_{PRF-CC} gives an optimistic, and ρ_{PRF-CC} a conservative result, as is shown in the next theorem.

<u>Theorem 5.2</u>. For π_{PRF-CC} as given by (5.1.4), ρ_{PRF-CC} as given by (5.1.5), and p as given by (2.3.1) or (3.3.1), $\rho_{PRF-CC} \leq p \leq \pi_{PRF-CC}$.

<u>Proof</u>. The phase structure functions are greater after cut cancellation than before from (4.2.4); thus

$$(5.1.6) \qquad \prod_{j=1}^{m} E\phi_j(\underset{\sim}{U}^{(j)}) \leq \prod_{j=1}^{m} E\phi_j^-(\underset{\sim}{U}^{(j)}),$$

so that $p \leq \pi_{PRF-CC}$ from (3.3.1), (5.1.3), and (5.1.4).

The ϕ_j^-, $j=1,\ldots,m$ are non-decreasing, and therefore the same properties of associated random variables used before[36] lead to the inequality

$$\prod_{j=1}^{m} E\phi_j^-(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)}) \leq E \prod_{j=1}^{m} \phi_j^-(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)}).$$

The equivalent system has the same reliability before and after cut cancellation by Theorem 4.1, i.e.

$$E \prod_{j=1}^{m} \phi_j^-(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)}) = E \prod_{j=1}^{m} \phi_j(\underset{\sim}{U}^{(1)}\underset{\sim}{U}^{(2)}\ldots\underset{\sim}{U}^{(j)}),$$

so that $\rho_{PRF-CC} \leq p$ from (3.3.1) and (5.1.5). □

The four bounds presented so far all presuppose that the phase reliability functions h_j or $\bar{h}_j$ are known for all m phases. Although to compute them is considerably easier than to compute the reliability function for the complete equivalent system, it may still be a formidable task. In the following section, therefore, bounds are studied which do not involve the phase reliability functions.

5.2 BOUNDS BASED ON PHASE BOUNDS

For coherent single-phase systems with independent components, Esary and Proschan [1963] have established two bounds on system reliability which can be computed without a knowledge of the reliability function. In one case, the system is expressed as a series structure of subsystems each of which consists of the components in a minimal cut set acting in parallel. The reliabilities of all subsystems are calculated separately and then multiplied together, the result being the _minimal cut lower bound_. In the other case, the system is expressed as a parallel structure of subsystems each of which consists of the components in a minimal path set acting in series. Again, the subsystem reliabilities are calculated separately, and then the reliability of the system is computed as if the subsystems were independent, resulting in the _minimal path upper bound_.[37] (The _minimal path sets_ of a coherent system are the minimal, in the set inclusion sense, combinations of components which by all functioning ensure the functioning of the system.)

These two bounds, when applied to each phase separately, can be used to approximate mission reliability in the multi-phase case. Let h_{UBj} and h_{LBj} denote the minimal path upper bound and the minimal cut lower bound, respectively, for phase configuration j, j=1,...,m. Using basically the same approach as before, and choosing as component

reliabilities the conditional component phase reliabilities π_{kj} in one case and the (unconditional) component reliabilities ρ_{kj} in the other, one obtains the approximations[38]

$$(5.2.1) \qquad \pi_{PUB} = \prod_{j=1}^{m} h_{UBj}(\pi_{1j},\ldots,\pi_{nj})$$

and

$$(5.2.2) \qquad \rho_{PLB} = \prod_{j=1}^{m} h_{LBj}(\rho_{1j},\ldots,\rho_{nj}),$$

which by the following theorem are bounds on mission reliability.

Theorem 5.3. For π_{PUB} as given by (5.2.1), ρ_{PLB} as given by (5.2.2), and p as given by (2.3.1) or (3.3.1), $\rho_{PLB} \leq p \leq \pi_{PUB}$.

Proof. The phase configurations are coherent, thus $h_{LBj} \leq h_j \leq h_{UBj}$, $j=1,\ldots,m$, by construction, and the inequalities

$$(5.2.3) \qquad \prod_{j=1}^{m} h_j(\pi_{1j},\ldots,\pi_{nj}) \leq \prod_{j=1}^{m} h_{UBj}(\pi_{1j},\ldots,\pi_{nj})$$

and

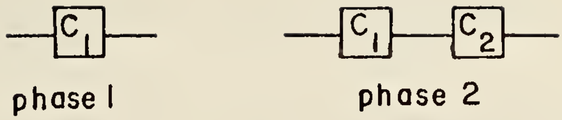
$$(5.2.4) \qquad \prod_{j=1}^{m} h_{LBj}(\rho_{1j},\ldots,\rho_{nj}) \leq \prod_{j=1}^{m} h_j(\rho_{1j},\ldots,\rho_{nj})$$

hold. Therefore $p \leq \pi_{PUB}$ from (5.1.1), (5.2.1) and Theorem 5.1, and $\rho_{PLB} \leq p$ from (5.1.2), (5.2.2) and Theorem 5.1. □

It is easy to see that if a different choice of component reliabilities is made, i.e. if the (unconditional) component reliabilities are used with the phase minimal path upper bounds, or the conditional component phase reliabilities with the phase minimal cut lower bounds, the resulting approximations are not bounds. For a mission with $m=1$ phases, obviously

$$\prod_{j=1}^{m} h_{UBj}(\rho_{1j},\ldots,\rho_{nj}) \geq p \geq \prod_{j=1}^{m} h_{LBj}(\pi_{1j},\ldots,\pi_{nj}),$$

and strict inequality may hold. On the other hand, for a phased mission with the block diagram



the exact mission reliability and the approximations are, in the established notation,

$$p = \rho_{12}\rho_{22} = \pi_{11}\pi_{12}\pi_{21}\pi_{22},$$

$$\prod_{j=1}^{2} h_{LBj}(\pi_{1j},\pi_{2j}) = \pi_{11}\pi_{12}\pi_{22},$$

$$\prod_{j=1}^{2} h_{UBj}(\rho_{1j},\rho_{2j}) = \rho_{11}\rho_{12}\rho_{22} = \pi_{11}\pi_{11}\pi_{12}\pi_{21}\pi_{22},$$

so that $\prod_{j=1}^{2} h_{UBj}(\rho_{1j},\rho_{2j}) \leq p \leq \prod_{j=1}^{2} h_{LBj}(\pi_{1j},\pi_{2j})$, and strict inequality holds if $0<\pi_{kj}<1$, $k=1,2$, $j=1,2$.

As before, cut cancellation can be performed prior to implementing the approximations (5.2.1) and (5.2.2). The resulting approximations corresponding to π_{PUB} and ρ_{PLB} are

(5.2.5) $$\pi_{PUB-CC} = \prod_{j=1}^{m} \bar{h}_{UBj}(\pi_{1j},\ldots,\pi_{nj})$$

and

(5.2.6) $$\rho_{PLB-CC} = \prod_{j=1}^{m} \bar{h}_{LBj}(\rho_{1j},\ldots,\rho_{nj}),$$

where $\bar{h}_{UBj}$ and $\bar{h}_{LBj}$ denote the minimal path upper bound and the minimal cut lower bound, respectively, for the simplified configuration of phase j, $j=1,\ldots,m$. Theorem 5.4 establishes that these approximations are bounds.

<u>Theorem 5.4</u>. For π_{PUB-CC} as given by (5.2.5), ρ_{PLB-CC} as given by (5.2.6), and p as given by (2.3.1) or (3.3.1), $\rho_{PLB-CC} \leq p \leq \pi_{PUB-CC}$.

<u>Proof</u>. The simplified phase configurations are coherent, thus $\bar{h}_{LBj} \leq \bar{h}_j \leq \bar{h}_{UBj}$, $j=1,\ldots,m$, by construction and the inequalities

(5.2.7) $$\prod_{j=1}^{m} h_j^-(\pi_{1j},\ldots,\pi_{nj}) \le \prod_{j=1}^{m} h_{UBj}^-(\pi_{1j},\ldots,\pi_{nj})$$

and

(5.2.8) $$\prod_{j=1}^{m} h_{LBj}^-(\rho_{1j},\ldots,\rho_{nj}) \le \prod_{j=1}^{m} h_j^-(\rho_{1j},\ldots,\rho_{nj})$$

hold. Therefore $p \le \pi_{PRF-CC}$ from (5.1.4), (5.2.5) and Theorem 5.2, and $\rho_{PRF-CC} \le p$ from (5.1.5), (5.2.6) and Theorem 5.2. □

Bounds π_{PUB-CC} and ρ_{PLB-CC} are the last to be considered here, although additional ones certainly could be found. Attention is now turned to a comparison and assessment of the bounds.

5.3 COMPARISON AND ASSESSMENT OF THE BOUNDS

The bounds presented in the previous two sections differ from each other in several respects, and it is not obvious which of them are suited best for a specific phased mission problem. It is therefore necessary to compare and assess them. From an applications point of view, the most significant criteria on which to base comparisons of bounds are felt to be precision, i.e. closeness to the exact reliability, and computational effort, i.e. cost of calculation. These criteria will be addressed in turn.

For single-phase systems, in order to obtain a rough idea of how system reliability responds to the achievement of a general, across-the-board level of component reliability, and to get an indication of the precision of bounds, it is often assumed that all components have the same probability of functioning. Then system reliability is a function of a single variable - component reliability - and can easily be exhibited. To use a similar approach for a system performing a phased mission, i.e. to assume that all conditional component phase reliabilities are equal, is somewhat more questionable but may still

provide an indication of the precision of bounds on mission reliability. The following example demonstrates this.

Example 5.1. Assume that in the mission of Example 1.1 all components have the same conditional phase reliability π in all phases, and consequently the same unconditional reliabilities $\rho_j = \pi^j$ in phase j, j=1,2,3. Then the exact mission reliability and the bounds on mission reliability, as a function of π, take on the numerical values given in Tables 5.1 and 5.2 below.

The tables show that for component reliabilities close to one, the lower bounds approximate the exact mission reliability quite closely whereas the same is not true for the upper bounds. This fact has been observed frequently in single phase systems.

π	p	π_{PRF}	π_{PRF-CC}	π_{PUB}	π_{PUB-CC}
0.40	0.002	0.025	0.058	0.036	0.077
0.50	0.011	0.078	0.141	0.119	0.190
0.60	0.045	0.187	0.274	0.284	0.366
0.70	0.137	0.364	0.454	0.526	0.584
0.80	0.337	0.596	0.661	0.782	0.797
0.90	0.668	0.834	0.857	0.955	0.948
0.95	0.854	0.932	0.938	0.991	0.987
0.99	0.978	0.989	0.990	1.000	0.999

Table 5.1. Exact mission reliability and upper bounds for the mission of Example 1.1.

π	p	ρ_{PRF}	ρ_{PRF-CC}	ρ_{PLB}	ρ_{PLB-CC}
0.40	0.002	$0.0^{4}64$	$0.0^{3}36$	$0.0^{5}30$	$0.0^{4}57$ 39
0.50	0.011	0.001	0.004	0.000	0.001
0.60	0.045	0.009	0.021	0.003	0.010
0.70	0.137	0.055	0.090	0.030	0.061
0.80	0.337	0.217	0.277	0.172	0.236
0.90	0.668	0.590	0.633	0.566	0.615
0.95	0.854	0.826	0.842	0.820	0.838
0.99	0.978	0.976	0.977	0.976	0.977

Table 5.2. Exact mission reliability and lower bounds for the mission of Example 1.1. □

The order among the bounds exhibited in Tables 5.1 and 5.2 is no coincidence and does not only hold for this particular example. The next theorem establishes some inequalities which are always valid.

<u>Theorem</u> <u>5.5</u>. For the bounds as given by (5.1.1), (5.1.2), (5.1.4), (5.1.5), (5.2.1), (5.2.2), (5.2.5), and (5.2.6), and p as given by (2.3.1) or (3.3.1), the following inequalities hold.

$$\rho_{PLB} \begin{array}{l} \le \rho_{PLB-CC} \\ \le \rho_{PRF} \end{array} \le \rho_{PRF-CC} \le p \le \pi_{PRF} \begin{array}{l} \le \pi_{PRF-CC} \le \pi_{PUB-CC} \\ \le \pi_{PUB} \end{array}$$

<u>Proof</u>. The proof consists of a separate demonstration for each inequality.

(1) $p \le \pi_{PRF}$ by Theorem 5.1.

(2) $\rho_{PRF-CC} \le p$ by Theorem 5.2.

(3) $\pi_{PRF} \le \pi_{PUB}$ from (5.1.1), (5.2.1), and (5.2.3).

(4) $\rho_{PLB} \le \rho_{PRF}$ from (5.1.2), (5.2.2), and (5.2.4).

(5) $\pi_{PRF-CC} \le \pi_{PUB-CC}$ from (5.1.4), (5.2.5), and (5.2.7).

(6) $\rho_{PLB-CC} \le \rho_{PRF-CC}$ from (5.1.5), (5.2.6), and (5.2.8).

(7) $\pi_{PRF} \le \pi_{PRF-CC}$ from (5.1.1), (5.1.4), and (5.1.6).

(8) $\rho_{PRF} \le \rho_{PRF-CC}$ from (4.2.4), (5.1.2), and (5.1.5).

Finally, since $\phi_j \le \bar{\phi}_j$, $j=1,\ldots,m$, from (4.2.4) and thus $h_{LBj} \le \bar{h}_{LBj}$, $j=1,\ldots,m$, the inequality

$$\prod_{j=1}^{m} h_{LBj}(\rho_{1j},\ldots,\rho_{nj}) \le \prod_{j=1}^{m} \bar{h}_{LBj}(\rho_{1j},\ldots,\rho_{nj})$$

holds, so that

(9) $\rho_{PLB} \le \rho_{PLB-CC}$ from (5.2.2) and (5.2.6). □

No general inequalities can be established between π_{PRF-CC} and π_{PUB}, and between ρ_{PLB-CC} and ρ_{PRF}. This is not too surprising. In the case of the two upper bounds, both cut cancellation and the use of phase upper bounds instead of phase reliability functions increase the apparent phase reliabilities; and in the case of the two lower bounds, cut cancellation and the use of phase lower bounds instead of phase reliability functions tend to balance each other. More formally, consider first a system where no cut cancellation is possible, i.e. $\bar{\phi}_j=\phi_j$, $j=1,\ldots,m$. If $h_{LBj}<h_j<h_{UBj}$ for some j, then $\pi_{PRF-CC}<\pi_{PUB}$ from (5.2.3), and $\rho_{PLB-CC}<\rho_{PRF}$ from (5.2.4). Next, consider a system with $h_{LBJ}=h_j=h_{UBj}$ for $j=1,\ldots,m$. If cuts can be cancelled in any one phase, i.e. if $\bar{\phi}_j>\phi_j$ for some j, then $\pi_{PRF-CC}>\pi_{PUB}$ and $\rho_{PLB-CC}>\rho_{PRF}$ from (4.2.4).[40] The relative magnitudes of these four bounds, however, may not only depend on the structure of the system under consideration, but also on the values of the component reliabilities.

This is the case in the system of Example 1.1 and can be seen by comparing the values of π_{PRF-CC}, π_{PUB}, ρ_{PLB-CC} and ρ_{PRF} for $\pi=0.4$ and $\pi=0.8$ in Tables 5.1 and 5.2.

The fact that π_{PUB} and π_{PUB-CC} also cannot be compared is somewhat counter-intuitive and unexpected, because it causes an unsymmetry in the string of inequalities of Theorem 5.5. However, it can be shown that even two single-phase systems with structure functions ϕ_1 and ϕ_2, $\phi_1 > \phi_2$, may have minimal path upper bounds h_{LB1} and h_{LB2} such that $h_{LB1} < h_{LB2}$. An example is a one-out-of-two system and a two-out-of-three system where all components have the same reliability p. In that case, $h_{LB1}(p) > h_{LB2}(p)$ for $0 < p \leq 0.8$, and $h_{LB1}(p) < h_{LB2}(p)$ for $0.9 \leq p < 1$. The mission of Example 1.1 shows a similar behavior, as can be seen by comparing the values of π_{PUB} and π_{PUB-CC} for $\pi=0.8$ and $\pi=0.9$ in Table 5.1.

As far as the computational effort required to calculate bounds is concerned, only a few statements valid in general can be made. One is that for any system performing a phased mission, less[41] effort is required to compute the m phase reliability functions separately than to compute the reliability function of the equivalent system; another, that phase bounds are easier to calculate then phase reliability functions. Cut cancellation simplifies all reliability calculations, but requires computational effort to be performed. This may be minimal in some cases (in particular when phase minimal cut lower bounds are used because then the minimal cuts of all phases have to be known explicitly), but cannot be neglected totally. On the whole, however, it is felt that the benefits of cut cancellation outweigh its costs.

The diagram below is an attempt to summarize the previous observations. Its comparisons may not hold in all cases, but do indicate what is usually true. The symbol $<$ stands for "requires less computational effort than."

$$\pi_{PUB\text{-}CC} < \pi_{PUB} < \pi_{PRF\text{-}CC} < \pi_{PRF}$$

p

$$\rho_{PLB\text{-}CC} < \rho_{PLB} < \rho_{PRF\text{-}CC} < \rho_{PRF}$$

Figure 5.1. A comparison of the computational effort required to calculate bounds.

5.4 AN ALGORITHM FOR THE "BEST" BOUND

Trying to select the best bound from those presented in this chapter is a difficult problem whose solution depends on the circumstances of each particular application and cannot be given in general. If one is interested in a conservative rather than an optimistic approximation, and if the system to be analyzed has components with uniformly high conditional reliabilities in all phases, then the qualitative comparisons of the previous section and the numerical values of Example 5.1 suggest that $\rho_{PLB\text{-}CC}$ is a good choice.

Since the above conditions are frequently encountered, and $\rho_{PLB\text{-}CC}$ hence might be used more often than other bounds, an algorithm for its computation is given below. This algorithm assumes that the survival function $\bar{F}_k(t) = P[T_k>t]$, $t\geq 0$, is known for each component C_k, $k=1,\ldots,n$, that each phase configuration is represented by a block diagram or a fault tree, and that the duration of the phases and thus the times t_j, $j=1,\ldots,m$, are given.

Algorithm for Computing ρ_{PLB-CC}.

(1) [42]For $k=1,\ldots,n$ and $j=1,\ldots,m$, compute ρ_{kj} from

$$\rho_{kj} = \bar{F}_k(t_j).$$

(2) For $j=1,\ldots,m$, find the minimal cut sets of phase j from the block diagram or the fault tree for that phase.[43]

(3) Perform cut cancellation according to the rule given in Section 4.2.

(4) For $j=1,\ldots,m$, denote the number of minimal cut sets remaining in phase j by $K(j)$, and the i-th minimal cut set in that phase by K_{ji}, $i=1,\ldots,K(j)$. Then compute ρ_{PLB-CC} from

$$\rho_{PLB-CC} = \prod_{j=1}^{m}\prod_{i=1}^{K(j)}[1 - \prod_{C_k \varepsilon K_{ji}}(1-\rho_{kj})].$$

The following example illustrates how the algorithm works.

Example 5.2. Suppose that for the mission of Example 1.1, a general expression for the lower bound ρ_{PLB-CC} is wanted. Using the algorithm described above, the following results are obtained:

(2) The minimal cut sets are

in phase 1 #{M,L}# {M,S}

in phase 2 {F} #{H,M}# #{H,T}# {M,L}

in phase 3 {F,M} {H,M} {H,T}

(3) The cut sets marked #{ }# above are cancelled.

(4) The minimal cut sets remaining are denoted by

$$K_{11} = \{M,S\},\ K_{21} = \{F\},\quad K_{22} = \{M,L\}$$

$$K_{31} = \{F,M\},\ K_{32} = \{H,M\},\ K_{33} = \{H,T\},$$

and the bound ρ_{PLB-CC} is given by

$$\rho_{PLB-CC} = [1-(1-\rho_{M1})(1-\rho_{S1})][1-(1-\rho_{F2})]$$

$$*[1-(1-\rho_{M2})(1-\rho_{L2})][1-(1-\rho_{F3})(1-\rho_{M3})]$$

$$*[1-(1-\rho_{H3})(1-\rho_{M3})][1-(1-\rho_{H3})(1-\rho_{T3})]. \ \square$$

This concludes the discussion of bounds based on reliabilities directly. In the next chapter, a reliability transformation is presented which permits the derivation of additional approximations and bounds.

6. HAZARD TRANSFORMS FOR PHASED MISSIONS

Recently, Esary and Hayne [1973] extended the scope of application of a simple reliability calculus of Rubinstein [1961, 1965] to coherent systems. This calculus uses an approximate hazard transform and leads to conservative approximations to system reliability. Its potential for use in the phased mission problem is explored here.

6.1 AN APPROXIMATE HAZARD TRANSFORM

The <u>hazard transform</u> of a system with reliability function $h(p_1,\ldots,p_n)$ is defined as

$$H(u_1,\ldots,u_n) = -\log h(p_1,\ldots,p_n) = -\log h(e^{-u_1},\ldots,e^{-u_n}),$$

where $u_k = -\log p_k$ is the <u>component hazard</u> of component C_k having reliability p_k, $k=1,\ldots,n$. Knowing the hazard transform of a system is equivalent to knowing its reliability function since

$$h(p_1,\ldots,p_n) = e^{-H(u_1,\ldots,u_n)} = e^{-H(-\log p_1,\ldots,-\log p_n)}.$$

The assumption that components perform independently is implicit in the definition of a hazard function, just as it is in the definition of a reliability function.

The <u>approximate hazard transform</u> H' considered by Esary and Hayne can be defined by the following rules:

(1) For a system consisting of a single component C_k, the approximate hazard transform is equal to the component hazard, i.e.

$$H' = u_k.$$

(2) For a system which is a combination of two modules (subsystems with disjoint sets of components) having approximate hazard transforms H_1' and H_2', the approximate hazard transform H' is

$$H' = H_1' + H_2' \quad \text{if the combination is series,}$$

$$H' = H_1'H_2' \quad \text{if the combination is parallel.}$$

So far, the rules define the approximate hazard transform only for systems that can be formed by successive series and parallel combinations of subsystems which have no components in common, i.e. for the class of simple systems considered by Lomnicki [1973]. To extend the definition to systems which are coherent but not necessarily simple, a third rule is needed. This rule makes use of the fact that any coherent system can be represented in terms of its minimal cut sets.

(3) For a coherent system with minimal cut sets $K_1,\ldots,K_\ell$ whose approximate hazard transforms are $H_1',\ldots,H_\ell'$, the approximate hazard transform H' is

$$H' = H_1' + H_2' +\ldots+ H_\ell'.$$

Esary and Hayne show[44] that the approximate hazard transform obtained in this way is conservative, i.e. indicates greater system hazard (less system reliability) than the exact transform. For further reference, this fact is noted as a theorem.

Theorem 6.1. For a coherent system with reliability function h, hazard transform H, and approximate hazard transform H' obtained according to the rules above, $H' \geq H$, and consequently $h' \leq h$, where $h' = e^{-H'}$. □

6.2 APPLICATION OF THE APPROXIMATE HAZARD TRANSFORM TO THE PHASED MISSION PROBLEM

Several approximations to the mission reliability of a multi-phased system can be derived using the approximate hazard transform defined in the previous section. One of them is discussed here in detail.

Suppose that cut cancellation has already been performed in a phased mission. Let H_j' be the approximate hazard transform of the simplified configuration of phase j, $j=1,\ldots,m$, and define an approximate hazard transform for the mission, H', by

(6.2.1) $$H' = H_1' + H_2' + \ldots + H_m'.$$

Then h' given by

(6.2.2) $$h' = e^{-H'} = e^{-(H_1' + H_2' + \ldots + H_m')}$$

is a conservative approximation to the mission reliability p, as is proved in the following theorem.

<u>Theorem 6.2</u>. For h' as given by (6.2.2) and p as given by (2.3.1) or (3.3.1), $h' \le p$.

<u>Proof</u>. Let $h_j'=e^{-H_j'}$, $j=1,\ldots,m$. Then $h' = \prod_{j=1}^{m} h_j'$ from (6.2.1) and (6.2.2). Since the phase configurations are coherent, then $h_j' \le h_j^-$, $j=1,\ldots,m$, by Theorem 6.1. Therefore, $\prod_{j=1}^{m} h_j' \le \prod_{j=1}^{m} h_j^-$, and the result follows from (5.1.5) and Theorem 5.2. □

An algorithm for computing h' consists of the following steps, where the notation of Section 5.4 is used:

(1) For $k=1,\ldots,n$ and $j=1,\ldots,m$, compute u_{kj} from

$$u_{kj} = -\log \rho_{kj} = -\log \bar{F}_k(t_j).$$

(2) For $j=1,\ldots,m$, find the minimal cut sets of phase j from the block diagram or the fault tree for that phase.

(3) Perform cut cancellation according to the rule of Section 4.2.

(4) Compute the approximate hazard transform for the mission from

$$H' = \sum_{j=1}^{m} \sum_{i=1}^{K(j)} \prod_{C_k \varepsilon K_{ji}} u_{kj}$$

(5) Compute the lower bound h' from

$$h' = e^{-H'}.$$

A comparison of this algorithm with the one presented in Section 5.4 indicates that the calculations of the bounds h' and ρ_{PLB-CC} require about the same amount of effort. Both are conservative, but h' is less precise than ρ_{PLB-CC}, as is established in Theorem 6.3 below. It is therefore questionable from an applications point of view whether h' can replace ρ_{PLB-CC} as the "best" lower bound for a phased mission. However, if all components of a system are assumed to have constant failure rates throughout each phase - as is often done for lack of better information about the distributions of the components' time to failures - the approximate hazard transform H' has the attractive feature that it is a polynomial in all of the phase durations. Thus it is well suited for parametric studies. An illustration for this is given after the assertion about the relative precision of h' and ρ_{PLB-CC} has been proved.

Theorem 6.3. For h' as given by (6.2.2), and ρ_{PLB-CC} as given by (5.2.6), $h' \leq \rho_{PLB-CC}$.

Proof. It suffices to note that in the calculation of ρ_{PLB-CC}, the exact reliability of each parallel subsystem corresponding to a

minimal cut set is used, whereas in the case of h', as a consequence of Theorem 6.1, a conservative approximation to the reliability of each such subsystem is the basis for the calculation. The result then follows from the fact that all other steps of the computation are equivalent. □

Example 6.1. Consider the mission of Example 1.1. Assume that the failure rate of component k in phase j is a constant r_{kj}, $k=F,H,L,M,S,T$, $j=1,2,3$, and let d_j be the duration of phase j, $j=1,2,3$. Then from step (1) of the algorithm above, the component hazards are

$$u_{kj} = r_{k1}d_1 + \ldots + r_{kj}d_j,$$

and the following general expression for the approximate hazard transform of the mission is obtained from step (4) of the algorithm:[45]

$$\begin{aligned} H' = {} & r_{M1}d_1 r_{S1}d_1 \\ & + (r_{F1}d_1+r_{F2}d_2) + (r_{M1}d_1+r_{M2}d_2)(r_{L1}d_1+r_{L2}d_2) \\ & + (r_{F1}d_1+r_{F2}d_2+r_{F3}d_3)(r_{M1}d_1+r_{M2}d_2+r_{M3}d_3) \\ & + (r_{H1}d_1+r_{H2}d_2+r_{H3}d_3)(r_{M1}d_1+r_{M2}d_2+r_{M3}d_3) \\ & + (r_{H1}d_1+r_{H2}d_2+r_{H3}d_3)(r_{T1}d_1+r_{T2}d_2+r_{T3}d_3). \end{aligned}$$

Now suppose that the duration of phase 2, d_2, is uncertain, and that a sensitivity analysis on it is desired. H' as a function of d_2 can be written as

(6.2.3) $$H'(d_2) = a + b*d_2 + c*d_2^2,$$

where

$$a = r_{M1}d_1r_{S1}d_1 + r_{F1}d_1 + r_{M1}d_1r_{L1}d_1$$

$$+ (r_{F1}d_1+r_{F3}d_3)(r_{M1}d_1+r_{M3}d_3)$$

$$+ (r_{M1}d_1+r_{M3}d_3)(r_{H1}d_1+r_{H3}d_3)$$

$$+ (r_{H1}d_1+r_{H3}d_3)(r_{T1}d_1+r_{T3}d_3),$$

$$b = r_{F2}(1+r_{M1}d_1+r_{M3}d_3)$$

$$+ r_{H2}(r_{M1}d_1+r_{M3}d_3+r_{T1}d_1+r_{T3}d_3)$$

$$+ r_{M2}(r_{L1}d_1+r_{F1}d_1+r_{F3}d_3+r_{H1}d_1+r_{H3}d_3)$$

$$+ r_{L2}r_{M1}d_1+r_{T2}(r_{H1}d_1+r_{H3}d_3),$$

$$c = r_{M2}r_{L2}+r_{F2}r_{M2}+r_{H2}r_{M2}+r_{H2}r_{T2}.$$

For a numerical illustration, assume that phase 1 lasts 30 minutes and phase 3 lasts 10 hours, and that the following failure rates (in hours^{-1}) are given:

Component	F	H	L	M	S	T
Phase 1	0.000	0.001	0.040	0.020	0.100	0.000
Phase 2	0.020	0.003	0.010	0.006	-	0.020
Phase 3	0.010	0.002	-	0.005	-	0.020

Then

$$a = 0.012030,$$

$$b = 0.023333 \text{ hours}^{-1},$$

$$c = 0.000258 \text{ hours}^{-2}.$$

For various durations of phase 2 (in hours), the approximate hazard transform for the mission, H', and the lower bound on mission reliability h', both rounded to three decimals, are shown below.

d_2	H'	h'
0	0.012	0.988
1	0.036	0.965
2	0.060	0.942
3	0.084	0.919
4	0.109	0.896
5	0.135	0.874
6	0.161	0.851
7	0.188	0.829
8	0.215	0.806
9	0.243	0.784
10	0.271	0.763 □

7. POSSIBLE EXTENSIONS AND REMAINING PROBLEMS

It was shown in this thesis how, under suitable assumptions, the phased mission problem can be formulated mathematically and transformed into an equivalent single-phase problem, and how exact mission reliabilities and approximations to them can be computed. The assumptions made, however, may not always be satisfied by realistic systems and missions which have to be analyzed. In particular, components may not perform independently,[46] failed components may be replaced, and the durations of the phases may not be known in advance.

Systems with interdependent components have been studied,[47] but so far no generally valid methods to model them seem to be available. In certain situations an approach similar to the one described in Chapter 3, i.e. the transformation of a system with interdependent components into an equivalent system whose synthetic components perform independently, may be feasible. Another approach might make use of the fact that several theorems on which lower bounds are based remain valid when component performances are positively dependent in the sense of association.[48]

As far as a replacement of failed components is concerned, it is felt that this feature can be incorporated into the model without causing major problems. If replacement is instantaneous at failure, it might simply be considered in the component's time to failure distribution; if replacement can occur only at the end of a phase, then the equivalent system may be modified to reflect this fact.

Example 6.1 indicated how uncertainties in the duration of the phases can be dealt with if component failure rates are constant

throughout the phases. Under these circumstances, and if phase durations are assumed to be random, the mean of the approximate hazard transform for the mission can be found, even without complete knowledge of the phase durations' distributions.[49]

As a final comment on the phased mission problem, it should be pointed out that even if all the extensions mentioned above can be incorporated into a model, practical use of it can only be made if all the necessary inputs are available. These inputs, the component reliabilities on one hand, and the functional organization of the system in the various phases of its mission on the other, are not always easy to obtain.

COMMENTS AND NOTES

[1] This term is used by Barlow and Proschan [1965].

[2] This definition of reliability is due to the Radio-Electronics Television Manufacturers Association [1955], as cited in Barlow and Proschan [1965], p. 6, and is widely accepted.

[3] Roughly, a system is coherent if its "performance is not impaired by an improvement in the performance of its components" [Esary and Marshall 1964, p. 459]. All two-terminal networks and all systems whose functional organization can be represented by a fault tree using AND and OR gates only are coherent. - Barlow and Proschan [1965] use the term "monotonic" instead, but "coherent" seems to be more widely accepted and will be used in this thesis.

[4] This approach was used before by Mine [1959].

[5] Barlow and Proschan [1965], pp. 196f.

[6] "Roughly...a device has a life if it functions continuously until some time of failure, and remains failed thereafter." [Esary and Marshall 1964, p. 459.]

[7] Among these are: components perform independently - components have exponential lives - only two states are recognized for components and systems.

[8] The method is described in Chapter 4.

[9] The manual section on phased missions is based on the work of C. Persels.

[10] Success paths and Muth's approach are briefly discussed in Section 1.4.

[11] Cf. the definition given above in Note 6.

[12] In the military, for instance, a communication network, the power plant of a ship, and a mine are systems which may be required to perform phased missions.

[13] Apologies are extended for this example to all firemen and all chemical engineers.

[14] Esary and Marshall [1964], Theorem 3.1, p. 461.

[15] Muth [1964], p. 2.

[16] Rubin [1964], p. 263.

[17] Expressing the life length as a random variable also permits by the proper choice of its distribution function, taking into account the operating conditions (the environment) which the system encounters.

[18] This is one of the classic assumptions mentioned before which are not very realistic but without which an exact reliability analysis is currently impossible.

[19] An example for a system which violates this assumption is an HF-communication network. Here the atmospheric conditions play an important factor in determining whether the system functions or not.

[20] A block diagram is a graphical model of the functional organization of components in a system. It provides a positive view of the system in that it indicates the combinations of functioning components which guarantee the functioning of the system.

[21] A fault tree is also a graphical model of the functional organization of a system, but in contrast to a block diagram it provides a negative view of the system because it indicates which combination of failed components cause failure of the system.

[22] Almost all engineering system are coherent. A ship with two captains could be an example for a system which is not coherent. Generally, an EXCLUSIVE OR gate in a fault tree indicates a non-coherent system.

[23] This follows immediately from the definition; cf. Esary and Proschan [1963], p. 192.

[24] Birnbaum, Esary, and Saunders [1961], pp. 66f.

[25] Esary and Marshall [1964], Theorem 3.1, p. 461.

[26] Cf. Figure 3.1. Component M^1, for instance, is common to all three subsystems.

[27] Such computational methods are, for instance, the inclusion-exclusion algorithm and pivotal decomposition.

[28] Cf. Fussell and Vesely [1972] and Vesely and Narum [1970] who describe programs for the analysis of fault trees.

[29] Barlow and Proschan [197_] Chapter 1, or Birnbaum, Esary, and Saunders [1961], Theorem 2.7.7.1, p. 65.

[30] Note, however, that as a result of cut cancellation the reliability of each phase configuration considered by itself increases.

[31] Cf. Examples 1.2 and 3.1 and the paragraphs preceding them.

[32] The subscript PRF is used mnemonically to indicate that these approximations are based on the phase reliability functions.

[33] These are discussed, for instance, in Barlow and Proschan [197_], Chapter 2, and in Esary, Proschan, and Walkup [1967]. From the latter paper, Theorem 2.1, Theorem 4.1, and Property (P4) are needed in this proof.

[34] Association is a special kind of positive dependence among several random variables. Performance state indicator variables are associated if the structure functions of any two coherent systems built from their corresponding components are positively correlated.

[35] The added subscript CC indicates that cut cancellation has been performed.

[36] Cf. the second part of the proof of Theorem 5.1.

[37] A detailed discussion of these bounds and proofs are given in Esary and Proschan [1963], Section 4, pp. 194-197.

[38] The subscript PUB stands for phase upper bounds, and the subscript PLB for phase lower bounds.

[39] The abbreviation $0.0^4 64$ stands for 0.000064.

[40] It is assumed here that all conditional component phase reliabilities are strictly positive and less than one.

[41] Terms which indicate a comparison are used here in the weak sense, i.e. "less" stands for "not more".

[42] Step (1) can be omitted if a general expression for the bound rather than a numerical value for it is needed.

[43] There exist computer programs which can perform this step. MOCUS, for instance, developed by Fussell, Henry, and Marshall [1974], is a program that finds the minimal cut sets of a system from its fault tree.

[44] Esary and Hayne [1973], Theorem 2.5, p. 12.

[45] Steps (2) and (3) of the algorithm are the same as in Example 5.2 and not repeated here.

[46] Interdependence among components may be caused, for instance, by common manufacturing processes or common operating conditions, or because the failure of one component increases the load on its neighbor.

[47] For instance by Esary and Marshall [1974].

[48] Cf. Remark 2.4 in Esary and Hayne [1973], p. 11.

[49] Equation (6.2.3) shows that for the particular mission considered $E\, H'(D_2)$ depends only on the first two moments of the random variable D_2.

REFERENCES

BARLOW, R. E. and PROSCHAN, F. (1965).
Mathematical Theory of Reliability. Wiley, New York

BARLOW, R. E. and PROSCHAN, F. (197_).
Statistical Theory of Reliability and Life Testing.
Volume I: Probability Models. To be published.

BIRNBAUM, Z. W., ESARY, J. D., and SAUNDERS, S. C. (1961).
Multi-Component Systems and Structures and Their Reliability.
Technometrics 3, 55-77.

ESARY, J. D. and HAYNE, W. J. (1973).
Properties of an Approximate Hazard Transform. Naval Postgraduate School Report NPS55EY73091A. To appear in Naval Res. Log. Quart.

ESARY, J. D. and MARSHALL, A. W. (1964).
System Structure and the Existence of a System Life.
Technometrics 6, 459-462.

ESARY, J. D. and MARSHALL, A. W. (1974).
Multivariate Distributions with Exponential Minimums.
The Annals of Statistics 2, 84-98.

ESARY, J. D. and PROSCHAN, F. (1963).
Coherent Structures of Non-Identical Components.
Technometrics 5, 191-209.

ESARY, J. D., PROSCHAN, F., and WALKUP, D. W. (1967).
Association of Random Variables, with Applications.
Ann. Math. Statist. 38, 1466-1474.

FUSSELL, J. D., HENRY, E. B., and MARSHALL, N. H. (1974).
MOCUS - A Computer Program to Obtain Minimal Sets from Fault Trees.
Aerojet Nuclear Company, Idaho Falls, Idaho.

FUSSELL, J. B. and VESELY, W. E. (1972).
A New Methodology for Obtaining Cut Sets for Fault Trees.
Trans. Amer. Nucl. Soc. 15, 262-263.

LOMNICKI, Z. A. (1973.
Two-Terminal Series-Parallel Networks. Adv. Appl. Prob. 4, 109-150.

MINE, H. (1959).
Reliability of Physical Systems. Transactions of the 1959 International Symposium on Circuits and Information Theory.

MOORE E. F. and SHANNON, C. E. (1956).
Reliable Circuits Using Less Reliable Relays. J. of the Franklin Institute 262, 191-208 and 281-297.

MUTH, E. J. (1964).
Reliability Assessment of Multiphase Missions. General Electric Company, Daytona Beach, Florida.

von NEUMANN, J. (1956).
Probabilistic Logics. Automata Studies, edited by C. E. Shannon and J. McCarthy. Princeton University Press, Princeton, New Jersey.

RADIO-ELECTRONICS-TELEVISION MANUFACTURES ASSOC. (1955).
Electronic Applications Reliability Review 3, 18.

RUBIN, J. C. (1964).
The Reliability of Complex Networks. Proceedings of the Aero-Space Reliability and Maintainability Conference.

RUBINSTEIN, D. (1961).
On the Estimation of System Reliability. Proceedings of the 1961 National Aerospace Electronics Conference, Dayton, Ohio, 262-266.

RUBINSTEIN, D. (1965).
On the Inference of System Reliability, Report I - Mathematical Models. General Electric Radio Guidance Operation, Report R65RG05.

U.S. NAVY STRATEGIC SYSTEMS PROJECTS OFFICE (1973).
Reliability Evaluation Program Manual. NAVORD OD 29304 Revision A.

VESELY, W. E. and NARUM, R. E. (1970).
PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree. Aerojet Nuclear Company, Idaho Falls, Idaho.

WEISBERG, S. A. and SCHMIDT, J. H. (1966).
Computer Technique for Estimating System Reliability. Proceedings of the 1966 Annual Symposium on Reliability. IEEE 7C26.

INITIAL DISTRIBUTION LIST

	NO. COPIES
Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
Library, Code 0212 Naval Postgraduate School Monterey, California 93940	2
Department of the Navy Pers 11b Washington, D.C. 20370	1
Chairman, Code 55 Department of Operations Research and Administrative Sciences Naval Postgraduate School Monterey, California 93940	2
Dokumentationszentrale der Bundeswehr (See) D-53 Bonn Friedrich-Ebert-Allee 34 Federal Republic of Germany	1
Marineamt -A1- D-294 Wilhelmshaven Federal Republic of Germany	1
German Military Representative USA/CA S1 StOffz 4000 Brandywine Street, N.W. Washington, D.C. 20016	1
Professor J. D. Esary, Code 55EY Department of Operations Research and Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
Professor J. K. Hartman, Code 55HH Department of Operations Research and Administrative Sciences Naval Postgraduate School Monterey, California 93940	1

Professor K. T. Marshall, Code 55MT 1
Department of Operations Research
and Administrative Sciences
Naval Postgraduate School
Monterey, California 93940

Professor J. J. von Schwind, Code 58VS 1
Department of Oceanography
Naval Postgraduate School
Monterey, California 93940

Professor F. R. Schwirzke, Code 61SW 1
Department of Physics and Chemistry
Naval Postgraduate School
Monterey, California 93940

Professor K. E. Woehler, Code 61WH 1
Department of Physics and Chemistry
Naval Postgraduate School
Monterey, California 93940

Dr. B. J. McDonald 1
Office of Naval Research
Arlington, Virginia 22217

Dr. S. M. Selig 1
Office of Naval Research
Arlington, Virginia 22217

Lieutenant Commander A. Cicolani SP1141 1
Strategic Systems Project Office
Department of the Navy
Washington, D. C. 20390

Professor E. J. Muth 1
College of Engineering
University of Florida
Gainesville, Florida 32611

Commander H. Ziehms, SMC 1691 1
Naval Postgraduate School
Monterey, California 93940